UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/729,852	12/05/2003	Gregory A. Girsham	1505-0157	8312

7590 08/16/2007

Harold C. Moore
Maginot, Moore & Beck LLP
Bank One Center/Tower
111 Monument Circle, Suite 3000
Indianapolis, IN 46204-5115

EXAMINER	
WEST, THOMAS CHARLES	

ART UNIT	PAPER NUMBER
3609	

MAIL DATE	DELIVERY MODE
08/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/729,852	GIRSHAM ET AL.	
	Examiner	Art Unit	
	Thomas West	3609	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 July 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 July 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Status of the Application

1. Claims 1-19 and 20(new) have been examined in this application. This is a Non-Final Office Action in response to the "Amendment" and "Remarks" filed on 7-23-07.

Claim Objections

2. Claims 1-12 are objected to because of the following informalities: The term "ANSI C12.19" is an industry standard or a trademark, which by nature, are subject to change in meaning and scope. Appropriate correction is required. The Office recommends amending the preamble so that a more generic term is used in place of "ANSI C12.19."

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The term "Decade4 table parameters" in line 5 of Claim 1 renders these claims indefinite because it appears that the parameters in the "Decade4 table" are industrial standards, which are subject to change. The Office

recommends amending the claims so that actual and, hence, permanent parameters are claimed.

Claim Rejections - 35 USC § 103

5. Claims 1-12 are rejected under U.S.C. 103(a) as being unpatentable over Hoffman et al, US Patent No. 5, 715, 390 in view of Matyas et al, US Patent No. 4,918,728, and further in view of Moore et al, US Patent No. 6,067,622.

Examiner's Note: The Examiner has pointed out particular references contained in the prior art of record within the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply. Applicant, in preparing the response, should consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

As per claim 1:

With regard to the limitations of *a security component for determining whether an externally generated access key is the same as an internally generated access key*, Hoffman explicitly teaches: "*The upgrade software program then processes the read secret software key and the read unique serial number of the meter with the stored authentication algorithm to generate at least one password. The password along with an upgrade command are presented to the meter where they are compared to the read-protected passwords in the RAM of the meter, and, if there is a match, then the upgrade*

command initiates the ROM codes for implementing one or more stored options or upgrades." (Hoffman, column 2, lines 54-62).

The referenced password generated above from the secret software key is externally generated and is equivalent to the "externally generated access key". The read-protected password above is equivalent to the "internally generated access key" to one skilled in the art at the time of the invention.

Moore teaches, the inputted purveyor install key is compared against the internally generated install key number series at inquiry step 32 (see at least column 9, lines 43-49). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Hoffman with the internally generated access install key to enhance security to prevent unauthorized data access operations.

With regard to the limitations of *a bypass component for enabling a data access operation by an external device without reference to Decade4 table parameters*, Hoffman explicitly teaches: "The upgrade command identifying the desired option or upgrade is programmed into the upgrade software program" (Hoffman, column 2, line 63-65).

The upgrade software program above sends a command identifying the desired option, which enables a data access operation for upgrading the meter through an external device (Hoffman, column 2, lines 62-64).

With regard to *without reference to Decade4 table parameters,* Hoffman teaches a system in terms of security features, it does not explicitly describe a system to bypass security. Maytas however teaches: "Protection From Non-System Generated Keys. The

method for coupling the control vector and key is such that CV checking is unable to detect a system generated key (via KGEN or GKS) from a non-system generated key. For this reason, a "back-door" method exists within the architecture for generating a keys and control vectors. It consists of defining a control vector "of choice" and a random number which is then represented as a key encrypted in the manner described under the architecture using the selected control vector. The so-called "back-door" method of key generation is primarily an annoyance, although in some cases cryptographic attacks would be possible if additional measures of defense were not taken in the architecture" (Matyas, column 15, lines 18-27 and 31-34).

The *Deacde4 table parameters* are the security limiting tables, which are part of the ANSI C12.19 standard where access permissions are used to limit table read or write access, although the exact means for granting access are not defined by the standard. The present invention involves a back-door or bypass method that goes around the ANSI C12.19 security features. Back-door or bypass security methods are well known in the art as exemplified by Maytas, which in this case, control vector checking is unable to detect a system generated key from a non-system generated key, much like what is being done in the current application. In light of Maytas, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate such a bypass of security features since this allows for meter calibration and upgrade that would otherwise be denied access.

As per claim 2:

With regard to the limitations of *a security component further comprising: a security key generator for generating a security key,* Hoffman explicitly teaches "an upgrade software program that reads the serial number from the RAM in the meter and reads the secret software key from the hardware key. The upgrade software program then processes the read secret software key and the read unique serial number of the meter with the stored authentication algorithm to generate at least one password" (Hoffman, column 4, lines 52-57).

The password generated above by the upgrade software program is equivalent to the "*security key generator*" to one skilled in the art at the time of the invention.

As per claim 3:

With regard to the limitations of *the security key generator generates the security key from variable data and data associated with the meter*, Hoffman explicitly teaches: "The upgrade software program reads the serial number from the RAM in the meter and reads the secret software key from the hardware key. The upgrade software program then processes the read secret software key and the read unique serial number of the meter with the stored authentication algorithm to generate at least one password" (Hoffman, column 2, lines 52-57).

"More specifically, the software key is a counter, which is decremented each time an upgrade is downloaded to a meter, so that only the number of upgrades purchased

can be enabled. The hardware key is a storage medium for the software key described above" (Hoffman, column 1, lines 41-46).

The password generated above consists of data associated with the meter, the meter's serial number and the software key being a counter, constitutes variable data.

As per claim 4:

With regard to the limitations of *the security key generator arithmetically combines the variable data and the data associated with the meter to generate the security key,* Hoffman explicitly teaches:

"The upgrade software program that reads the serial number from the RAM in the meter and reads the secret software key from the hardware key. The upgrade software program then processes the read secret software key and the read unique serial number of the meter with the stored authentication algorithm to generate at least one password" (Hoffman, column 2, lines 52-57).

"The following described authentication algorithm accepts:

(1) the sixteen byte secret and protected keying variable;

(2) the sixteen byte meter serial number; and

(3) the one byte option code;

and returns a 4 byte authentication password."

"In accordance with the authentication algorithm of the present invention, an array of 33 bytes, B(i,j), is defined where i, 1 □ I □ 33, is the byte number and, j, 0 □ j □

7, specifies the bits within byte i. The least significant bit (LSB) is specified by j=0; and the most significant bit (MSB) is specified by j=7" (Hoffman, column 5, lines 7- 18).

The references above show arithmetically combining variable data, the software key and the data associated with the meter, the meter's serial number, through the use of the authentication algorithm, which is equivalent to the "*security key*" to one skilled in the art at the time of the invention.

As per claim 5:

With regard to the limitations of *a security component further comprising: an access key generator for generating an access key from the security key,* Hoffman explicitly teaches: "The password is generated by processing a software key and a serial number of the meter with an authentication program by a processor external to the meter." (Hoffman, column 5, lines 47- 50).

"The described authentication algorithm returns a 4 byte authentication password" (Hoffman, column 4, lines 7- 12).

As per claim 6:

With regard to the limitations of *the access key generator augments the security key before generating the access key,* Hoffman explicitly teaches: "The 4 byte password resulting from the cycling of initialized array B (FIG. 3), as described above, is shown in FIG. 4. A 4 byte password resulting from the cycling of initialized array B (FIG. 3), with the exception of the option byte being set to the value 2 instead of 1, is shown in FIG. 5.

It will be appreciated that the change in the option status has resulted in a significant change in the password. This is also the case for a small change in the serial number or the key." (Hoffman, column 5, lines 65-68 and column 6, lines 3-6).

The references above clearly shows that the authentication algorithm has augmented the security of the system, since any small change in the input to the algorithm results in a significant change in the resulting password.

As per claim 7:

With regard to the limitations of *the security component further comprising: An access key comparator for comparing the access key generated by the access key generator to an access key received from an external device,* Hoffman explicitly teaches: "The password along with an upgrade command are presented to the meter where the password presented is compared to the read-protected password in the RAM of the meter in step 80, and, if there is a match, then the upgrade command initiates the ROM codes for implementing one or more stored options or upgrades in step 81." (Hoffman, column 4, lines 57-63).

As per claim 8:

With regard to the limitations of *a data access monitor for monitoring data access operations performed by the external device and resetting the access key comparator in response to a data access being performed by the external device.* Hoffman explicitly teaches: "In accordance with the present invention, ROM includes codes for

implementing one or more stored options or upgrades. It will be appreciated that these options or upgrades are stored in the meter at the factory and can be utilized only when purchased and enabled as described herein. Each meter has a unique serial number stored in RAM. In the present example, the serial number is 16 bytes long and includes bit-flags (i.e., an option byte) indicating which options have already been enabled. Each option which is not enabled must be requested and a password verified before it can be utilized. It is an important feature of the present invention that the password be based on the serial number, so that the same password cannot simply be recorded and played back to another meter. Further, the password cannot be used to upgrade more than the option(s) selected (and purchased) " (Hoffman, column 2 lines 16-29).

"The upgrade command initiates the ROM codes for implementing one or more stored options or upgrades in step 81. The upgrade command identifying the desired option or upgrade is programmed into the upgrade software program." (Hoffman, column 4, lines 61-65).

"After 330 cycles, the contents of bytes B30, B31, B32, and B33 are defined to be the password corresponding to the specific key, meter serial number, and option. The authentication algorithm being known will not in of itself allow recovery of the secret key. Further, if a single bit is changed in the serial number, the option byte, or the key, then the authentication password will change in a difficult to predict fashion" (Hoffman, column 5, lines 46-54).

"It will be appreciated that the change in the option status has resulted in a significant change in the password. This is also the case for a small change in the serial number or the key" (Hoffman, column 6, lines 3-6).

It is clear from the references above that the upgrade command and the counter function as a data access monitor since each option which is not enabled must be requested and a password verified before it can be utilized. The authentication algorithm referenced above functions as the reset mechanism since it prevents further upgrades through a significant change in the password should any small change occur in the option status, key, or serial number of the meter. A change in this externally generated password would not match the meter's internally generated password preventing further data access to the meter, functioning as reset of the access key comparator of the current invention.

As per claim 9:

With regard to the limitations of *a unlock timer for timing an interval corresponding to a data access operation and for resetting the access key comparator in response to a data access being performed by the external device.* Hoffman explicitly teaches: "The counter is decremented each time an upgrade is downloaded to a meter, so that only the number of upgrades purchased can be enabled" (Hoffman, column 4, lines 65-67).

The counter above functions as an unlock timer providing limited data access for a period based on the number of upgrades purchased that can be enabled. As

mentioned above, the authentication algorithm functions as the reset mechanism since it prevents further upgrades through a significant change in the password should any small change occur in the option status, key, or serial number of the meter.

As per claim 10:

With regard to the limitations of the bypass component enables a single data access operation by the external device. Hoffman explicitly teaches: "The upgrade command identifying the desired option or upgrade is programmed into the upgrade software program" (Hoffman, column 2, line 62-64).

"The password is generated by processing a software key and a serial number of the meter with an authentication program by a processor external to the meter" (Hoffman, column 4, lines 47-50).

The upgrade software program above sends a command identifying the desired option, which enables a data access operation for upgrading the meter through an external device (Hoffman, column 2, lines 62-64).

"The counter is decremented each time an upgrade is downloaded to a meter, so that only the number of upgrades purchased can be enabled" (Hoffman, column 4, lines 65-67).

It should be clear from the above references, that the counter above functions as an unlock timer providing limited data access for a period based on the number of upgrades purchased that can be enabled and that upgrading is done through an external device.

As per claim 11:

- With regard to the limitations of *the security component and bypass component are implemented by a procedure.* Hoffman explicitly teaches: "The upgrade command identifying the desired option or upgrade is programmed into the upgrade software program" (Hoffman, column 4, line 63-65).
    - The security component and the upgrade software program are equivalent per Claim 2's rejection and it is well known in the art that software programs contain and are developed through the use of procedures.
    - The bypass component and the upgrade software program are equivalent per Claim 1's rejection and it is well known in the art that software programs contain and are developed through the use of procedures.

As per claim 12:

With regard to the limitations of *the procedure is a computer program executed by a processor in the utility meter.* Hoffman explicitly teaches: "The password along with an upgrade command are presented to the meter where they are compared to the read-protected passwords in the RAM of the meter, and, if there is a match, then the upgrade command initiates the ROM codes for implementing one or more stored options or upgrades (Hoffman, column 4, lines 57-63).

The comparison of passwords is obviously done, to someone skilled in the art, by the meter's internal processor and the processor also responds thereafter to the upgrade command.

6. Claims 13-19 and 20(new) are rejected under U.S.C. 103(a) as being unpatentable over Hoffman et al, US Patent No. 5, 715, 390 in view of Matyas et al, US Patent No. 4,918,728, in view of Moore et al, US Patent No. 6,067,622 and further in view of Lee et al, US Patent Publication No. 2004/0264701.

As per claim 13:

Hoffman/Maytas teach the limitations as shown above. Hoffman/Maytas do not teach the following limitation, but Lee does: *receiving a request for a security* key. Lee teaches: "In a second step, the ultra-wideband terminal of the transmission part receives, in response to the request, a security key transmitted from the ultra-wideband terminal of the reception part" (see at least paragraph 12).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Hoffman/Maytas with the security key of Lee to enhance security to prevent unauthorized data access operations.

With regard to the limitation of *generating a security key.* Hoffman teaches, (see at least, Hoffman column 4, lines 52-57);

With regard to the limitation of *generating an access key from the security key* (see at least Hoffman, column 5, lines 47- 50);

Hoffman/Maytas teach the limitations as shown above. Hoffman/Maytas do not teach the following limitation, but Moore does: *comparing the generated access key to an externally generated access key* (see at least Moore column 9, lines 43-49). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Hoffman/Maytas with Moore to enhance security to prevent unauthorized data access operations.

With regard to the limitation of *enabling a data access operation to occur without reference to security access tables* (see at least Hoffman, column 2, line 63-65).

As per claim 14:

With regard to the limitation of *arithmetically combining variable data with data associated with a utility meter to generate the security key* (see at least Hoffman, column 2, lines 52-57).

As per claim 15:

With regard to the limitation of *augmenting the security key before generating the access key* (Hoffman, column 5, lines 65-68 and column 6, lines 3-6).

As per claim 16:

With regard to the limitation of *Monitoring for a data access operation by an external device in response to the comparison of the access keys being the same* (Hoffman, column 2 lines 16-29).

As per claim 17:

With regard to the limitation of *timing a data access interval* (see at least Hoffman, column 4, lines 65-67);

With regard to the limitation of *resuming security processing with reference to security tables in response to the data access interval time expiring* (see at least Hoffman, column 4, lines 65-67).

As per claim 18:

With regard to the limitations of *generating the access key with an encryption function,* Hoffman explicitly teaches: "After 330 cycles, the contents of bytes B30, B31, B32, and B33 are defined to be the password corresponding to the specific key, meter serial number, and option. The authentication algorithm being known will not in of itself allow recovery of the secret key. Further, if a single bit is changed in the serial number, the option byte, or the key, then the authentication password will change in a difficult to predict fashion" (Hoffman, column 5, lines 47-54).

The authentication algorithm being known does not in and of itself allow recovery of the secret key, is indicative of and the result of, to on skilled in the art, to an encryption function.

As per claim 19:

With regard to the limitations of *generating the access key with a hashing function*. Hoffman explicitly teaches: It will be appreciated that the change in the option status has resulted in a significant change in the password. This is also the case for a small change in the serial number or the key." (Hoffman, column 6, lines 3-6).

This result is indicative of and the result of, to one skilled in the art, to a hashing function, where the fundamental property of all hash functions is that if two hashes, according to the same function, are different, then the two inputs are different in some way.

As per claim 20 (new):

With regard to the limitation of performing a data access operation without reference to the security tables (see at least Hoffman, column 2, line 63-65).

Response to Arguments

7. Applicant's arguments filed on 7-23-07 have been fully considered but they are not persuasive. Applicant's arguments will be addressed in sequential order as they were set forth in the "Remarks" section on 7-23-07.

8. The drawings submitted on 7-23-04 are in compliance with 37 C.F.R. 1.121(d) and are accepted.

9. The applicant's arguments regarding the rejection of claim 1 under 35 U.S.C. 112 first and second paragraphs have been accepted and the prior rejections are withdrawn.

10. The applicant's arguments regarding the rejection of claim 13 under 35 U.S.C. 101 have been accepted and the rejection is withdrawn.

11. Applicant argues that the limitation of claim 1 is not taught or suggested by Hoffman. Hoffman teaches a method of gaining access to an electricity meter through the comparison of an external password with an internal password, which implicitly solves the nature of the problem as a whole; gaining access to the meter is key to any further operations. "The test for an implicit showing is what the combined teachings, knowledge of one of ordinary skill in the art and the nature of the problem as a whole have suggested to those of ordinary skill in the art", MPEP 2143.01.

Applicant further argues that Matyas teaches away from the claimed invention. Maytas explicitly raises the issue of a "back-door" method of generating keys in which CV checking is unable to detect a system generated key from a non-system generated key. Maytas characterizes this back-door method as a type of cryptographic attack, which in general attempts to circumvent security measures and are well known in the information security art. Applicant also circumvents built-in security tables by using a "back-door" or bypass method of access.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas West whose telephone number is 571-270-1236. The examiner can normally be reached on M-R 7:30am - 5pm., est ALT Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Reagan can be reached on 571-272-6710. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Thomas West
Patent Examiner
August 8, 2007

Signature: Thomas West

JAMES REAGAN
SUPERVISORY PATENT EXAMINER